KOPELOWITZ OSTROW P.A.
Kristen Lake Cardoso (SBN 338762)
cardoso@kolawyers.com
Jeff Ostrow (pro hac vice forthcoming)
ostrow@kolawyers.com
Kenneth Grunfeld (pro hac vice forthcoming)
grunfeld@kolawyers.com
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
Counsel for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

Zachary Richmond, *individually and on behalf of all others similarly situated*, Plaintiff, v. **Vivendi Ticketing US LLC d/b/a See Tickets**, Defendant.	**Case No.** **PLAINTIFF'S CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Zachary Richmond, individually and on behalf of all similarly situated persons, alleges the following against Vivendi Ticketing US LLC d/b/a See Tickets ("Vivendi" or "Defendant") based on personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents, as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Vivendi for its failure to properly secure and safeguard Plaintiff's and other similarly situated Vivendi customers' sensitive information, including full names, addresses, account numbers, and payment card information ("Private Information").

2. Defendant is a leader in the global ticketing market, providing customers with

access to purchase tickets for a variety of events in the United States and around the world.

3. Upon information and belief, former and current Defendant customers are required to entrust Defendant with Private Information without which Defendant could not perform its regular business activities, in order to obtain services from Defendant. Defendant retains this information for at least many years and even after the consumer relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. In May of 2023, Defendant was alerted to unusual activity on certain of its e-commerce websites. Specifically, Defendant asserts that unauthorized parties inserted multiple instances of malicious code into a number of its e-commerce checkout pages, resulting in unauthorized access to, and acquisition of, certain customer payment card information, including that belonging to Plaintiff.[1] The Private Information was impacted that was provided by customers (including Plaintiff) through purchases made on the Defendant's website between February 28, 2023 and July 2, 2023 (the "Data Breach").[2]

6. On or about September 6, 2023, Defendant filed a data breach notice with the Maine Attorney General's office, reporting that over 323,498 customers were affected.

7. On that same day, Defendant began notifying affected individuals, including Plaintiff. *See* the "Notice Letter".[3] Otherwise, Defendant has taken no steps to inform Plaintiff and Class Members that their Private Information had been compromised even though Defendant knew or should have known and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

8. Defendant failed to adequately protect Plaintiff's and Class Members' Private Information. This Private Information was compromised due to Defendant's negligent and/or

[1] https://www.seetickets.us (last visited Sept. 22, 2023).
[2] *Id.*
[3] Attached as **Exhibit A**.

careless acts and omissions and their utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in making fraudulent purchases and exploiting or stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Importantly, this is the second major data breach that See Tickets has reported in less than a year's time. In October of 2022, Defendant reported a different data breach that impacted over 400,000 customers' payment card data.[4]

10. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

11. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by its IT vendors to ensure that the PRIVATE INFORMATION of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

12. Plaintiff and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they should be entitled to injunctive and other equitable relief.

13. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct.

[4] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/86fc7ff5-d406-422d-889c-d4e6abd62177.shtml (last visited Sept. 20, 2023).

In addition to fraud, these injuries include: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

14. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

II. PARTIES

15. Plaintiff Zach Richmond, is, and at all times mentioned herein was, an individual citizen and resident of Chicago, Illinois. Plaintiff received a Notice of Data Breach letter (attached hereto as **Exhibit A**), via U.S. mail.

16. Defendant Vivendi Ticketing US LLC, d/b/a See Tickets, is a Delaware corporation with its principal place of business located at 6380 Wilshire Boulevard, Suite 900, Los Angeles, California 90048. Vivendi Ticketing US LLC is a wholly owned subsidiary of Vivendi Village, which is the live entertainment and ticketing business unit of Vivendi SE, the Vivendi media and communications group.

III. JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the state of Texas and have different citizenship from Vivendi, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A)

18. This Court has jurisdiction over Vivendi because Vivendi operates in this District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Vivendi has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. *Defendant's Business*

20. Defendant is one of the leaders in the global ticketing market.

21. It's parent company, Vivendi SE, is a French mass media holding company with reported revenues in the first quarter of 2022 as $2.76 billion.[5] Vivendi's business is growing in part because the success of it See Tickets brand.[6]

22. Plaintiff and Class Members are current and former Vivendi customers.

23. As a condition of receiving its products and/or services, Vivendi requires that its customers, including Plaintiff and Class Members, entrust it with highly sensitive personal information, including:

- Email address;
- Name;
- Address;
- Zip Code;
- Payment card information;
- Payment card expiration date; and
- CVV number.

24. The information held by Defendant in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted data of Plaintiff and Class Members.

---

[5] *See Press Release,* Vivendi (April 25, 2022), *available at* https://www.vivendi.com/wp-content/uploads/2022/04/20220425_VIV_PR_Vivendi-Q1-2022-revenues.pdf.

[6] See Annual Report – Universal Registration Document 2021, Vivendi, available at https://www.vivendi.com/wp-content/uploads/2022/04/20220404_VIV_Rapport-annuel-2021_VA.pdf (last visited Sept. 20, 2023).

25. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiff and Class Members, that the data collected from them as a condition of obtaining products and/or services would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

26. At the time of the Data Breach, Defendant promised its customers that it would not share this information with non-Vivendi owned companies third parties.[7] Other than sharing with financial organizations to process orders, and with social media companies for marketing, the See Tickets privacy policy states:

> See Tickets will only process your data with 3rd party organizations if you have consented to hearing news and data from them. See Tickets will specify who the data will be shared with during the process of purchasing a ticket. The 3rd parties may, from time to time, send you data about the event you have purchased tickets for, as well as further data for similar shows and events.
>
> All 3rd party organizations must adhere to the General Data Protection Act 2018.

27. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

28. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

29. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendant has a legal duty to keep

[7] *See US Privacy Policy,* See Tickets, *available at* https://misc.seetickets.us/privacy/#informationwemaycollect (last visited Sept. 10, 2023).

consumer's Private Information safe and confidential.

30. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

B. *The Data Breach*

32. Based on the Notice Letter filed by Defendant and sent to Plaintiff and Class Members, it was alerted to activity indicating unauthorized access by a third party to event checkout pages on the See Tickets website in May of 2023.

33. Defendant then learned that an unknown third party had obtained unauthorized access to Defendant's data starting in February of 2023. Defendant was only able to stop the unauthorized access in July of 2023, two (2) months after initially learning of the Data Breach and five (5) months after the Data Breach started.

34. In or around early September 2023, Defendant issued Notice Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in a data breach. This means that Plaintiff and Class Members had no idea their Private Information had been compromised for seven (7) months after Defendant first learned about the Data Breach.

35. The Notice Letter then attached information about identity protection, and listed generic steps that victims of data security incidents can take, such as examining account statements, getting a copy of a free annual credit report, or implementing a fraud alert or security freeze.

36. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

37. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

38. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed. Moreover, Defendant failed to exercise due diligence in selecting its IT vendors or deciding with whom it would share Private Information.

39. Plaintiff further believes his Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type. Moreover, following the Data Breach, Plaintiff has experienced significant fraud.

C. *Defendant Acquires, Collects, and Stores Plaintiff's and the Class's Private Information.*

40. As a condition to obtain products and/or services from Vivendi, Plaintiff and Class Members were required to give their Private Information to Defendant.

41. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to perform its services.

42. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

43. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

44. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members or by exercising due diligence in selecting its IT vendors and properly auditing those vendor's security practices.

45. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing it.

46. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

D. *Defendant Knew or Should Have Known of the Risk of Cyber Attacks.*

47. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting businesses that collect and store Private Information, like Defendant, preceding the date of the breach.

48. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they control. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

49. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[8]

50. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

[8] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (https://notified.idtheftcenter.org/s/), at 6.

51. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems, or those of its vendors, were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

52. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

53. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

54. Additionally, as companies became more dependent on computer systems to run their business,[9] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[10]

55. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

56. In the Notice Letter, Defendant offers to cover identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of

[9] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited Sept. 20, 2023).

[10] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited Sept. 20, 2023).

ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff and Class Members' Private Information. Moreover, once this service expires, Plaintiff and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

57. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and Class Members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

58. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

59. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Private Information is stolen—fraudulent use of that information and damage to victims may continue for years.

E. *Value of the Private Information*

60. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[12]

61. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[13]

62. For example, Private Information can be sold at a price ranging from $40 to $200.[14]

---

[11] 17 C.F.R. § 248.201 (2013).
[12] *Id.*
[13] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Sept. 22, 2023).
[14] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

63. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

64. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[16]

F. *Vivendi Failed to Comply with FTC Guidelines.*

65. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

66. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security

[15] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

67. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. These FTC enforcement actions include actions against financial institutions, like Defendant.

70. As evidenced by the Data Breach, Vivendi failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Vivendi's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

71. Vivendi was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. *Vivendi Failed to Comply with Industry Standards.*

72. Experts studying cyber security routinely identify ecommerce platforms as being particularly vulnerable to cyberattacks because of the value of the Private Information which they

collect and maintain.

73. Several best practices have been identified that a minimum should be implemented by ecommerce providers like Defendant, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

74. A number of industry and national best practices have been published and should be used as a go-to resource when developing a business' cybersecurity standards. The Center for Internet Security ("CIS") released its Critical Security Controls. The CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia.

75. Other best cybersecurity practices that are standard in the ecommerce industry include installing appropriate malware detection software; monitoring and setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

76. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

H. *Vivendi Breached Its Duty to Safeguard Plaintiff's and Class Members' Private Information.*

77. In addition to its obligations under federal and state laws, Vivendi owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being

compromised, lost, stolen, accessed, and misused by unauthorized persons. Vivendi owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

78. Vivendi breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Vivendi's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

e. Failing to sufficiently train its employees and vendors regarding the proper handling of its customers Private Information;

f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

79. Vivendi negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

80. Had Vivendi remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information

storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

I. *Common Injuries & Damages*

81. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including fraud as well as: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

J. *The Data Breach Increases Victims' Risk of Identity Theft.*

82. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

83. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

84. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

85. One such example of criminals piecing together bits and pieces of compromised

Private Information for profit is the development of "Fullz" packages.[17]

86. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

K. *Loss of Time to Mitigate Risk of Identity Theft and Fraud*

87. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

88. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendant's Notice Letter instructs, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

89. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and resecuring their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

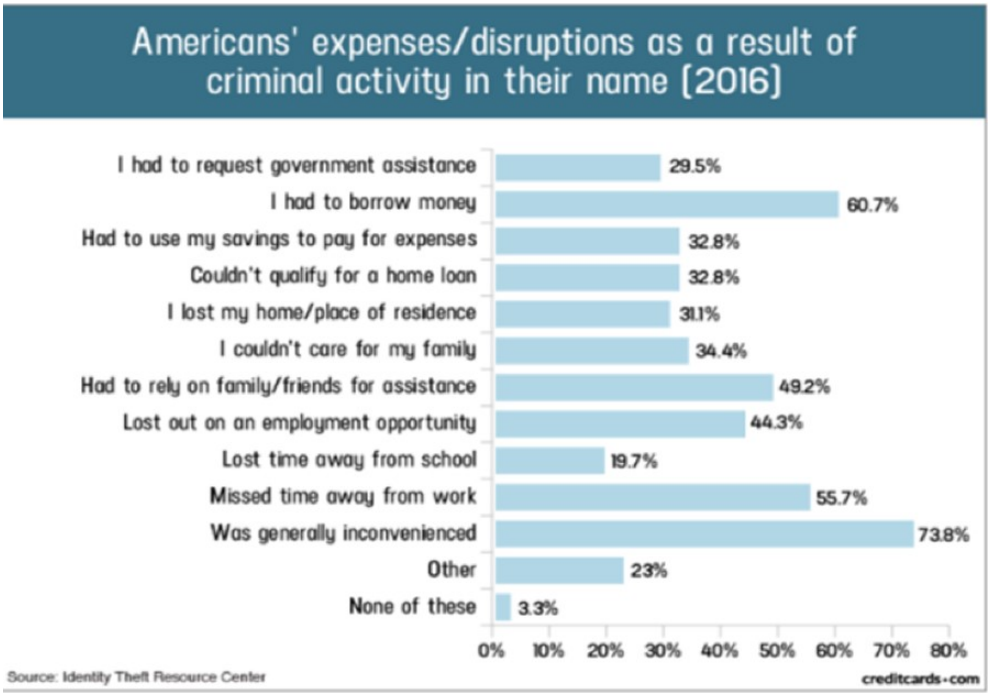
90. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit

[17] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/ medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited 9/20/2023).

record."[18]

91. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[19]

92. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[20]



93. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches

[18] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[19] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.
[20] Jason Steele, "Credit Card and ID Theft Statistics," Oct. 24, 2017, https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[21]

L. *Diminution Value of Private Information*

94. Private Information is a valuable property right.[22] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

95. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[23]

96. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[24,25]

97. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[26]

98. Conversely sensitive Private Information can sell for as much as $363 per record on the dark web according to the Infosec Institute.[27]

99. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an

---

[21] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. GOV'T ACCOUNTABILITY OFFICE, June 2007, https://www.gao.gov/ new.items/d07737.pdf ("GAO Report").

[22] *See, e.g.*, Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009).

[23] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[24] https://datacoup.com/ (last visited Aug. 11, 2023).

[25] https://digi.me/what-is-digime/ (last visited Aug. 11, 2023).

[26] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

[27] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

economic loss.

100. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

101. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to thousands of individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

102. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

M. ***Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary.***

103. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes.

104. Such fraud may go undetected until debt collection calls commence months, or even years, later.

105. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

106. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for

Defendant's failure to safeguard their Private Information.

N. *Loss of the Benefit of the Bargain*

107. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for products and/or services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the product and/or service and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

O. *Plaintiff's Experience*

108. Plaintiff Zachary Richmond has been a See Tickets customer for at least 4 years. He has a current account and last made a purchase in March of 2023.

109. Plaintiff was required to provide his Private Information to Defendant, including his name, email address, home address, and payment card data.

110. At the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

111. Plaintiff is very careful about sharing and protecting his Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

112. Plaintiff received the Notice Letter, by U.S. mail, from Defendant. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties.

113. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including cancelling his credit card and obtaining another one, changing passwords and resecuring his own computer

network, and checking his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

114. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) lost or diminished value of his Private Information; (ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iii) invasion of privacy; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

115. Plaintiff further suffered actual injury. In April and May, he had 3 different fraudulent charges for hundreds of dollars on his credit card; the same card he provided to Defendant. That fraud required him to cancel the credit card. In addition, he has experienced an increase in spam emails, which, upon information and belief, was caused by the Data Breach and only began following the Data Breach.

116. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence. Further, as the sole provider of tickets to events that the Plaintiff plans to attend in the future, he knows that he is required to continue to use See Tickets in the future for ticketing needs.

117. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

118. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

119. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ACTION ALLEGATIONS

120. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

121. Specifically, Plaintiff proposes the following class definitions, subject to amendment as appropriate:

> **Nationwide Class**
> All individuals in the United States whose Private Information was disclosed in the Data Breach (the "Class").
>
> **Illinois Subclass**
> All individuals in the state of Illinois whose Private Information was disclosed in the Data Breach (the "Illinois Subclass").

122. Excluded from the Class and Subclass are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

123. Plaintiff reserves the right to modify or amend the definition of the proposed Class and/or Florida Subclass, as well as add subclasses, before the Court determines whether certification is appropriate.

124. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

125. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes that the proposed Class includes thousands of individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

126. Commonality. There are questions of law and fact common to the Class which

predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Vivendi engaged in the conduct alleged herein;

b. When Vivendi learned of the Data Breach;

c. Whether Vivendi's response to the Data Breach was adequate;

d. Whether Vivendi unlawfully shared, lost, or disclosed Plaintiff's and Class Members' Private Information;

e. Whether Vivendi failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether Vivendi's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Vivendi's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Vivendi owed a duty to Class Members to safeguard their Private Information;

i. Whether Vivendi breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether Vivendi had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

l. Whether Vivendi breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether Vivendi knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of Vivendi's misconduct;

o. Whether Vivendi's conduct was negligent;

p. Whether Vivendi was unjustly enriched;

q. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

r. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

127. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of Vivendi. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

128. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

129. Predominance. Vivendi has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Vivendi's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

130. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in

the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Vivendi. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

131. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Vivendi has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

132. Finally, all members of the proposed Class are readily ascertainable. Vivendi has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Vivendi.

CLAIMS FOR RELIEF

COUNT I

Negligence and Negligence Per Se

(On Behalf of Plaintiff and the Class)

133. Plaintiff restates and realleges paragraphs 1 through 132 above as if fully set forth herein.

134. Defendant requires its customers, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing services.

135. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business of soliciting its services to its clients and its clients' customers, which solicitations and services affect commerce.

136. Plaintiff and Class Members entrusted Defendant with their Private Information

with the understanding that Defendant would safeguard their information.

137. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

138. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

139. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

140. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

141. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Vivendi and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Vivendi with their confidential Private Information, a necessary part of being customers of Defendant.

142. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

143. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

144. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' Private Information it was no longer required to retain pursuant to regulations.

145. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

146. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

147. Defendant breached its duties, pursuant to the FTC Act, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former customers' Private Information it was no longer required to retain pursuant to regulations; and

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

148. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

149. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

150. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

151. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

152. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

153. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial industry.

154. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

155. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

156. It was therefore foreseeable that the failure to adequately safeguard Class

Members' Private Information would result in one or more types of injuries to Class Members.

157. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

158. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

159. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

160. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

161. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

162. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

163. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for

unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

164. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

165. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

166. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

167. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

168. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II

Breach Of Implied Contract

(On Behalf of Plaintiff and the Class)

169. Plaintiff restates and realleges paragraphs 1 through 132 above as if fully set forth herein.

170. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of receiving services from Defendant.

171. Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

172. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

173. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

174. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

175. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

176. In accepting the Private Information of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

177. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of

which relate to the Data Breach.

178. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

179. Plaintiff and Class Members paid money and provided their Private Information to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

180. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

181. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

182. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

183. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

184. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

185. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

186. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide

adequate credit monitoring to all Class Members.

COUNT III

Unjust Enrichment

(On Behalf of Plaintiff and the Class)

187. Plaintiff restates and realleges paragraphs 1 through 132 above as if fully set forth herein.

188. This count is pleaded in the alternative to the Breach of Implied Contract claim above (Count II).

189. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

190. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

191. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

192. Defendant acquired Private Information through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

193. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information to Defendant or obtained services from Defendant.

194. Plaintiff and Class Members have no adequate remedy at law.

195. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

196. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

197. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

198. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV

VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT

(By Plaintiff on Behalf of the Illinois Subclass)

199. Plaintiff restates and realleges paragraphs 1 through 132 above as if fully set forth herein and brings this claim on behalf of himself and the Illinois Subclass (the "Class" for the purposes of this count).

200. In Illinois, the "Consumer Fraud and Deceptive Business Practices Act" 815 Ill.

Comp. Stat. 505/1, *et seq*., prohibits "unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact or the use or employment of any practice described in Section 2 of the 'Uniform Deceptive Trade Practices Act' . . . ."

201. Plaintiff and the Illinois Subclass members were injured by Defendant's deceptive misrepresentations, concealments, and omissions, and these misrepresentations, concealments and omissions were material and deceived Plaintiff and the Illinois Subclass. Because Plaintiff and the Illinois Subclass members relied on CVS's misrepresentations, concealments, and omissions when purchasing products and services, they were injured at the time of purchase.

202. Defendant does business in Illinois and engaged in deceptive acts and practices in connection with the business in Illinois and elsewhere in the United States.

203. The products and services purchased by Plaintiff and the Illinois Subclass members were "consumer items" as that term is defined under the Illinois Consumer Fraud Act.

204. Defendant engaged in unfair and deceptive acts in violation of 815 Ill. Comp. Stat. 505/2 when it misrepresented and deceptively concealed, suppressed, and/or omitted the material information known to it, which has caused damage and injury to Plaintiff and the Illinois Subclass members. Plaintiff and the Illinois Subclass members were injured by Defendant's unfair and deceptive acts at the time of purchasing the products and services.

205. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard Private Information;

b. failure to audit, monitor, or verify the integrity of data security procedures implemented by third parties with whom Defendant shared Private Information;

b. failure to make only authorized disclosures of current and former customers' Private

Information;

c. failure to disclose that their data security practices were inadequate to safeguard Private Information from theft; and

d. failure to timely and accurately disclose the Data Breach to Plaintiff and Class members.

206. Defendant deceived its customers, which created a likelihood of confusion or of misunderstanding in violation of the Act. It knew or should have known that all consumers who purchased the products and services would be impacted by its misrepresentations and omissions.

207. These deceptive acts occurred in a course of conduct involving trade and commerce in Illinois and throughout the United States.

208. Defendant intended Plaintiff and the Illinois Subclass members to rely on its deceptive acts, which proximately caused actual injury and damage to Plaintiff and the Illinois Subclass members.

209. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have been harmed and have suffered damages including, but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and actual fraud, including an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

210. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff and Class members have been damaged and are entitled to recover an order providing declaratory and injunctive relief and reasonable attorneys' fees and costs, to the extent permitted by law.

211. Plaintiff and the Illinois Subclass members would not have purchased, or would have paid less for, the products and services but for the material misrepresentations and omission as described in this Complaint.

COUNT V

VIOLATION OF ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT

(By Plaintiff on Behalf of the Illinois Subclass)

212. Plaintiff restates and realleges paragraphs 1 through 132 above as if fully set forth herein and brings this claim on behalf of himself and the Illinois Subclass (the "Class" for the purposes of this count).

213. Plaintiff brings this claim on behalf of herself the Illinois Subclass.

214. The Illinois Deceptive Trade Practices Act ("UDTPA"), 815 Ill. Comp. Stat. 510/2, *et seq*., prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact."

215. 815 ILCS 510/2 provides in pertinent part that a "person engages in a deceptive trade practice when, in the course of his or her business, vocation, or occupation," the person does any of the following: "(5) represents that goods or services have . . . uses, benefits or quantities that they do not have . . .; (7) represents that goods or services are of a particular standard, quality, or grade or that goods are a particular style or model, if they are of another; . . . [or] (12) engages in any other conduct which similarly creates a likelihood of confusion or misunderstanding."

216. Defendant violates this prohibition by deceiving consumers into believing they adequately protect Private Information. This creates a likelihood of confusion or of misunderstanding in violation of the Act.

217. Defendant intended that Plaintiff and each of the other Illinois Subclass members would reasonably rely upon the material misrepresentations and omissions concerning the true nature of the products and services.

218. Defendant's concealment, omissions, and other deceptive conduct were likely to deceive and cause misunderstanding and/or in fact caused Plaintiff and each of the other Illinois Subclass members to be deceived in a course of conduct involving trade and commerce in Illinois and throughout the United States.

219. Defendant's deceptive acts proximately caused actual injury and damage to Plaintiff and the Illinois Subclass members.

220. Plaintiff and the Illinois Subclass members would not have purchased, or would have paid less for, the products and services but for the material misrepresentations as described in this Complaint.

221. Defendant intended Plaintiff and the Illinois Subclass members to rely on its deceptive acts.

COUNT VI

DECLARATORY JUDGMENT

(On Behalf of Plaintiff and the Class)

222. Plaintiff restates and realleges paragraphs 1 through 132 above as if fully set forth herein.

223. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

224. Defendant owes a duty of care to Plaintiff and Class Members which required it to adequately secure Private Information.

225. Defendant still possesses Private Information regarding Plaintiff and Class Members.

226. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of Private Information, and remains at imminent risk that further compromises of the Private Information will

occur in the future.

227. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' Private Information; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

228. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect customers' Private Information, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members, and

b. Order Defendant to comply with its explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures.

229. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

230. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued, especially considering the Data Breach is the second breach of Defendant's network and systems in less than two years. Therefore, Plaintiff will likely be

subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by finally employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

231. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and customers whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class and Subclass, pursuant to Federal Rule of Civil Procedure 23;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide

to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training

and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Dated: September 22, 2023.

Respectfully submitted,

/s/ Kristen Lake Cardoso
Kristen Lake Cardoso (SBN 338762)
Jeff Ostrow*
Kenneth Grunfeld*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
cardoso@kolawyers.com
ostrow@kolawyers.com

Counsel for Plaintiff and the Proposed Class

**Pro Hac Vice* application forthcoming